STATEMENT OF THE CLAIMS

1 - 72 (cancelled)

73. (new) A method of authenticating data and providing a dated audit trail, said method comprising:

(a) storing copies of a plurality of data items at a first location;

(b) generating a first data file at the end of a predetermined dated audit period, the first data file comprising a respective hash value of each said plurality of stored data items;

(c) generating a single hash value of said first data file, the single hash value corresponding to said predetermined dated audit period;

(d) transmitting said single hash value to a second location remote from said first location, via an information technology communications network;

(e) creating at said remote location a second data file for said predetermined dated audit period, said second data file comprising said single hash value and one or more additional data items relating to said single hash value;

(f) generating a hash value for said second data file, said hash value for said second data file corresponding to said predetermined dated audit period;

(g) publishing said hash value for said second data file in a dated journal of record published in numerous copies and held in separate public libraries, wherein the published hash value for said second data file corresponds to said predetermined dated audit period;

(h) at a date subsequent to the publishing of (g), generating a hash value for said second data file; and

(i) comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal, whereby if the hash value generated in step (h) is identical to the hash value published in said dated journal said second data file is authenticated.

74. (new) A method according to claim 73, wherein:

said first data file contains at least one identifier selected from the group consisting of a file name, a path name, a file size and a time stamp.

75. (new) A method according to claim 73, wherein:

least one of said first data items comprises a message to be transmitted from a sender to a receiver.

76. (new) A method according to claim 75, further comprising:

the sender generating a first hash value of said message;

the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message;

the sender encrypting said first secret key with a second secret key;

the sender transmitting to the receiver said encrypted message, said encrypted first secret key and said first hash value;

the sender transmitting said second hash value and said second secret key to a third party;

the third party storing the transmitted second hash value and second secret key for audit purposes;

the receiver receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message;

the receiver transmitting the purported copy of said second hash value to the third party;

the third party determining whether the purported copy matches said second hash value; and

the third party then releasing said second key if a match is so determined.

77. (new) A method according to claim 76, wherein:

the first secret key is symmetric and the second secret key is asymmetric.

78. (new) A method according to claim 73, wherein:

said first location is a predetermined audit location that stores data items supplied thereto over the predetermined dated audit period, and the first data file generated in (a) comprises respective hash values of the data items stored in said predetermined audit location at the end of the predetermined dated audit period.